IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Robert Nazzal	Art Unit	: 2134
Serial No.	: 10/701,157	Examiner	: Jason K. Gee
Filed	: November 3, 2003	Conf. No.	: 5548
Title	: FEEDBACK MECHANISM TO MINIMIZE FALSE ASSERTIONS OF A NETWORK INTRUSION		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF ON BEHALF OF ROBERT NAZZAL

Please charge the Brief fee of **$255** and please apply any other charges or credits to Deposit Account No. 06-1050.

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: August 08, 2008

(1) Real Party in Interest

The real party in interest in the above application is Mazu Networks, Inc.

(2) Related Appeals and Interferences

Appellant is not aware of any appeals or interferences related to the above-identified patent application.

(3) Status of Claims

This is an appeal from the decision of the Primary Examiner in a final office action dated **February 8, 2008**, finally rejecting claims 1-25, all of the claims in the application. Appellant filed a Notice of Appeal on **June 9, 2008**. Claims 1-25 are the subject of this Appeal.

(4) Status of Amendments

Appellant filed a Reply to the Final Office Action. In the advisory action, the examiner indicated entry of the Reply. No amendments were made to the claims in response to the final rejection. All previously filed amendments have been entered.

(5) Summary of Claimed Subject Matter

Claim 1

Appellant's claim 1 is directed to a graphical user interface rendered on a display associated with an intrusion detection system. "***The event details screen 310 provides further detail about events.***"[1] "***Referring to FIG. 19, intrusion detection system 10 as in FIG. 1 includes .. ..***"[2]

Inventive features of Appellant's claim 1 include a field that depicts a summary of anomalies identified as part of an event that is detected in a network, the summary indicating event severity details of the event. "***The event details screen 310 provides further detail about events. In particular, the event details screen 310 provides a summary 312 of the anomalies***

[1] Specification page 12, lines 12-13.
[2] Id. 32, line 27.

identified as part of the event. In the summary 312 the event severity as well as details such as the Date/Time, Source, Destination, and Protocol used are displayed along with values for these items."[3]

Inventive features of Appellant's claim 1 also include an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time. "***The event details screen 310 also includes an alert action region 314 where a user can "snooze" future alerts related to this event for a fixed period of time (for example, while the event is being addressed).***"[4]

Claim 10

Appellant's claim 10 is directed to a method. See original claim 10.

Inventive features of Appellant's claim 10 include providing an operator with a list of events identified by an intrusion detection system, within the list of events being information indicating event severity, with event severity determined for an event, by the event having a percentage relationship to an established threshold for issuing an event notification. "***The process provides 319 an operator with a list of events identified by the intrusion detection system. Within the list of events is information that indicates event severity, with severity determined based on an event having a percentage relationship to an established threshold for issuing an event notification, as discussed above.***"[5]

Inventive features of Appellant's claim 10 also include displaying details of a selected one of the events to a user. "***For instance, the event details region 316 allows a user to select "details" that will show details about the selected anomaly.***"[6]

Inventive features of Appellant's claim 10 also include providing on a graphical user interface a snooze control to allow a user to snooze future alerts related to the selected event. This feature is supported similar to the analogous feature of claim 1.

---

[3] Specification page 51, lines 12-18.
[4] Id. lines 21-24.
[5] Id lines 25-30.
[6] Id. lines 16-18.

Claim 22

Claim 22 is directed to a computer program product residing on a computer readable medium for producing a graphical user interface for an intrusion detection system. This feature is supported by the analogous feature of claim 1 and claim 22, as originally filed.

Inventive features of Appellant's claim 22 include instructions to render a graphical user interface on an output device. "***Referring to FIG. 30, to view the details of an event, a user can click on the line-item in the overview graphical user interface 302 and launch an event details screen 310.***"[7]

Inventive features of Appellant's claim 22 also include a field that depicts a summary of anomalies identified as part of an event that is detected in a network, the summary indicating event severity details of the event. This feature is supported similar to the analogous feature of claim 1.

Inventive features of Appellant's claim 22 also include an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time. This feature is supported similar to the analogous feature of claim 1.

(6) Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-9 and 22-25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper US Patent Application Publication 2002/0069200 (Cooper), and in view of Symantec's Symantec Antivirus for Macintosh SAM, 1994, (Symantec).

2. Claims 10-14 and 18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper and Symantec, and further in view of Billhartz US Patent No. 6,986,161 (Billhartz).

3. Claims 15-17 and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, and Billhartz, and further in view of Porras US Patent No. 6,321,338 (Porras).

[7] Specification page 53, lines 10-13.

4. Claim 19 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, Billhartz, and further in view of Central Point's Central Point Anti-Virus-Virus detection, Removal and Prevention, 1991 (Central Point).

5. Claim 20 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper, Symantec, Billhartz, and further in view of Kuroshita US Patent No. 5,550,807 (Kuroshita)

(7) Argument

Obviousness

"It is well established that the burden is on the PTO to establish a prima facie showing of obviousness, *In re Fritsch*, 972 F.2d. 1260, 23 U.S.P.Q.2d 1780 (C.C.P.A., 1972)."

In *KSR Intl. Co. v. Teleflex Inc.*, 127 S.Ct. 1727 (2007), the Supreme Court reversed a decision by the Court of Appeal's for the Federal Circuit decision that reversed a summary judgment of obviousness on the ground that the district court had not adequately identified a motivation to combine two prior art references. The invention was a combination of a prior art repositionable gas pedal, with prior art electronic (rather than mechanical cable) gas pedal position sensing. The Court first rejected the "rigid" teaching suggestion motivation (TSM) requirement applied by the Federal Circuit, since the Court's obviousness decisions had all advocated a "flexible" and "functional" approach that cautioned against "granting a patent based on the combination of elements found in the prior art."

In *KSR* the Supreme Court even while stating that: "the Court of Appeals drew the wrong conclusion from the risk of courts and patent examiners falling prey to hindsight bias," warned that: "a factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning."

> The Court of Appeals, finally, drew the wrong conclusion from the risk of courts and patent examiners falling prey to hindsight bias. A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex*

> *post* reasoning. See *Graham*, 383 U. S., at 36 (warning against a "temptation to read into the prior art the teachings of the invention in issue" and instructing courts to "'guard against slipping into the use of hindsight'" (quoting *Monroe Auto Equipment Co. v. Heckethorn Mfg. & Supply Co.*, 332 F. 2d 406, 412 (CA6 1964))). Rigid preventative rules that deny factfinders recourse to common sense, however, are neither necessary under our case law nor consistent with it.

With respect to the genesis of the TSM requirement, the Court noted that although "As is clear from cases such as Adams[8], a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. Although common sense directs one to look with care at a patent application that claims as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known."

"The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Gordon*, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984).

> Although the Commissioner suggests that [the structure in the primary prior art reference] could readily be modified to form the [claimed] structure, "[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Laskowski*, 10 U.S.P.Q. 2d 1397, 1398 (Fed. Cir. 1989).

"The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of

[8] United States v. Adams, 383 U. S. 39, 40 (1966)

making the combination." *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 488 (Fed. Cir. 1984).

> Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under Section 103, teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) (emphasis in original, footnotes omitted).

"The critical inquiry is whether 'there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.'" *Fromson v. Advance Offset Plate, Inc.*, 225 U.S.P.Q. 26, 31 (Fed. Cir. 1985).

(1) Claims 1-9 and 22-25 are patentable over Cooper and Symantec.

Claims 1, 3, 5-9, 22 and 24

For the purposes of this appeal only, Claims 1, 3, 5-9, 22 and 24 stand or fall together. Appellant's claim 1 is representative of this group of claims.

Claim 1 requires the features of a graphical user interface including "a field that depicts a summary of anomalies identified as part of an event that is detected in a network, the summary indicating event severity details of the event; and an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time.

The examiner argues that "**Cooper teaches a graphical user interface for an intrusion detection system, the graphical user interface comprising: a field that depicts a summary of anomalies identified as part of a event ... .**" Applicant disagrees.

The examiner uses Cooper's Fig. 26 as an instance that depicts the claimed feature of a field that depicts a summary of anomalies. However, neither in Fig. 26 nor in any of the other interfaces does Cooper depict "summary of anomalies identified as part of an event that is detected in a network, the summary indicating event severity details of the event.'

Appellant's claimed feature is directed to, e.g., the summary of anomalies depicted in bottom portion of the pane as "Anomalies detected" of FIG. 30 (shown below). The event however, is depicted in 312 of FIG. 30, an example of which is "Worm propagation suspected" (subject matter of claim 4).

In contrast, Cooper Fig. 26 depicts a table that has various rules displayed in a "Rules" column and a type of event in the "Type" column. Cooper itself refers to Fig. 26 as an "events summary" and does not summarize anomalies that generated the event.

The examiner admits that: "**Cooper does not explicitly teach an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time,**" and thus relies on Symantec. Specifically, the examiner argues: "**A snooze for future alerts is taught Symantec though, such as in pages 4-9 and 5-6, wherein an event may be allowed to continue, and an alert may be prevented from appearing in the future.**" Appellant contends that Symantec does not suggest any of the features of claim 1 and in particular: "a control to permit a user to snooze future alerts related to the event in the summary for a period of time."

Appellant's FIG. 30 is an example of the feature of the control to permit a user to snooze future alerts related to the event in the summary and is depicted below:

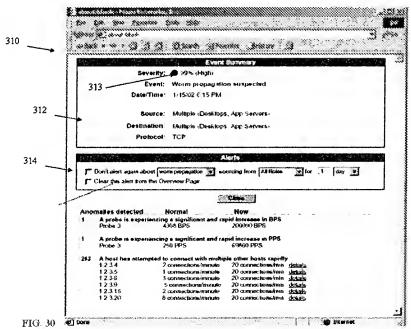
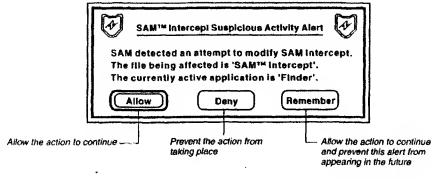


FIG. 30

In contrast, with Appellant's snooze feature depicted above, the so called "snooze feature of Symantec" that the examiner relies on is depicted below:

Figure 4-8



Unlike the claimed feature of "a control to permit a user to snooze future alerts related to the event in the summary for a period of time, the Symantec dialog box depicted above permits a user to choose whether or not to let the SAM allow an action to continue or prevent the action from taking place. That is, the dialog in Symantec has an "Allow" control, which is not a snooze control, and a "Deny" control, which is also not a snooze control.

Symantec also includes a "Remember" control that the examiner argues corresponds to the claimed feature.[9] The "Remember" control, unlike Appellant's claimed feature, allows the action to continue, but as stated in Symantec: "**Allow the action to continue and prevent this alert from appearing in the future.**"[10] Therefore, the Remember control, as with the Allow and Deny controls, does not suggest the feature of: "a control to permit a user to snooze future alerts related to the event in the summary." Moreover, the Remember control also does not operate allow to snooze futures alert for a "period of time." Thus, because Symantec's Remember control does not suggest either one or both of these properties of the claimed snooze control, it cannot when taken with Cooper suggest the claimed invention.

---

[9] Final Action page 2. "The applicant also argues that the combination does not teach a snooze function. However, Symantec teaches this by showing the 'remember' function, which allows an action to continue for a certain period of time."

[10] Symantec Figure 4-8.

Motivation to combine

The examiner also argues that: "**One of ordinary skill in the art would have been motivated to perform such an addition, as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious, and it would be more convenient to the user. Symantec teaches in 5-6 that not all suspicious activity alerts necessarily means there is malicious activity.**" Applicant contends that this motivation is nothing more than an exercise in *ex post* reasoning. Moreover, for the reasons pointed out above, the Symantec control would not be useful when combined with Cooper. Neither the "Allow" nor "Deny" controls suggest the claimed limitation, whereas the "Remember" control would permit what could appear to be innocuous anomalies to be ignored forever and erroneously result in a potentially serious network intrusion.

The Supreme Court in *KSR Intl. Co. v. Teleflex Inc.*, 127 S.Ct. 1727 (2007), even while stating that: "the Court of Appeals drew the wrong conclusion from the risk of courts and patent examiners falling prey to hindsight bias," warns that: "a factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning."

> The Court of Appeals, finally, drew the wrong conclusion from the risk of courts and patent examiners falling prey to hindsight bias. A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning. See *Graham*, 383 U. S., at 36 (warning against a "temptation to read into the prior art the teachings of the invention in issue" and instructing courts to "'guard against slipping into the use of hindsight'" (quoting *Monroe Auto Equipment Co. v. Heckethorn Mfg. & Supply Co.*, 332 F. 2d 406, 412 (CA6 1964))). Rigid preventative rules that deny factfinders recourse to common sense, however, are neither necessary under our case law nor consistent with it.

The examiner lays no basis for his conclusion that "**as some anomalies are not necessarily a sign of malicious activity. If this is the case, it would be beneficial to snooze these alerts, as they are not malicious.**" Neither Cooper nor Symantec discloses: "a field that depicts a summary of anomalies identified as part of an event" in the first instance. Nor does either of the references or any combination of their teachings describe: "an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time." Neither Cooper nor Symantec, as pointed out above, lay any basis for snoozing anomalies.

Therefore, the examiner's motivation to combine these references provides a clear example of *ex post* reasoning, that is, application of improper hindsight reconstruction, because the examiner could have only gleaned the advantages of the novel combination of elements set forth in claim 1, after reference to Appellant's claims and/or specification.

It has long been recognized that motivation to combine is effectively destroyed when the combination destroys the intent, purpose and function of one of the references. Here, the examiner argues that the Remember control in Symantec corresponds to the claimed snooze features. However, as pointed out above the Remember control does not snooze an anomaly but instead allows an action to continue forever unless the user somehow edits another file (an exceptions list) to change properties of the action.

The problem with this approach is that many of such anomalies can occur during the time that the user first "Remembers" the action, decides that maybe that was not a good idea, finds the action that was remembered, finds the exceptions list and edits the properties of the action, all of which assumes that the user can remember and identify which action that was remembered in the first instance is the cause of problems in the network that the user and system employing the invention is monitoring. Appellant submits that the Remember function is not equivalent to the claimed snooze functionality and that any modification of Cooper with the Remember function of Symantec would lead to more problems than it would solve.

Therefore, the examiner's argument in response to Appellant's challenge to motivation to combine that:

> **The applicant also argues that the combination does not teach a snooze function. However, Symantec teaches this by showing the 'remember' function, which allows an action to continue for a certain period of time. These may be later edited in time, if the user actually deems them suspicious or malicious, as taught by Symantec on 5-7, and thus, would be useful with the Cooper combination. Therefore, the combination teaches all the claimed limitations. This would be useful, as stated earlier, as not all suspicious activity alerts necessarily mean there is malicious activity; therefore, it would be advantageous to snooze these alerts to deal with later in case they really are issues.**

is clearly in error. The Remember function neither permits a user to snooze future alerts related to the event in the summary because neither reference suggests "a field that depicts a

summary of anomalies identified as part of an event," nor permits this to occur for a period of time. In Symantec the Remember function cannot be edited by the user, but the user can edit an exceptions list. However, despite the ability to edit the exceptions list these teachings do not meet the claim limitation of "a period of time" because there is no period that can be specified by the Remember control, which otherwise would need to be edited by a user in order to resume alerting the user.

Accordingly, no combination of these references suggests all of the features of claim 1.

Claims 2 and 23

For the purposes of this appeal only, Claims 2 and 23 stand or fall together. Appellant's claim 2 is representative of this group of claims.

Claim 2 requires the feature that "the snooze control feature is selected based on event types and roles of hosts." The examiner in response to Applicant's argument stated:

> **As per claim 2, the applicants argue that Cooper does not teach alerts based on grouping or roles of hosts. However, as cited in the previous office action, security policies based on roles of hosts are taught in Cooper in paragraph 100 and 158.**
>
> **Paragraph 100 teaches wherein policy may be based on communities of hosts, servers, subnets and firewalls, as well as service level. Also, as seen in table A in paragraph 86, communites of hosts are grouped together when they have similar functions/roles.**

Whether or not Cooper's "communities of hosts" correspond to roles of hosts, it does not follow from the examiner's argument that: "**However, as cited in the previous office action, security policies based on roles of hosts are taught in Cooper in paragraph 100 and 158.**" that Cooper at the cited passages teach alerts based on grouping or roles of hosts. Symantec being directed to a stand-alone application would not be concerned with grouping or roles *per se* and therefore no combination of Cooper with Symantec would suggest the features of claim 2.

Moreover, claim 2 requires that the features of the snooze control feature is selected based on the types and roles of hosts. Nothing in Symantec suggests that the dialog in figure 4-8 changes in any manner based on any consideration in Symantec, much less the types and roles of hosts.

Claims 4 and 25

For the purposes of this appeal only, Claims 4 and 5 stand or fall together. Appellant's claim 4 is representative of this group of claims.

Claim 4 recites that "... an event details region of the graphical user interface depicts anomalies that were used to classify the event." The examiner argues in response that: "**As per claim 4, Cooper does indeed teach that GUIs are used to depict anomalies that were used to classify the event, in Figure 12. The disposition, such as an invalid url, probable scan, are anomalies.**" Appellant believes that the examiner meant to refer to Fig. 21, not Fig. 12. Neither Fig. 21 nor Fig. 12 however depicts anomalies, but instead those figures depict alerts generated by Cooper's system. Appellant maintains that Cooper teaches events, but did not teach anomalies used to classify the events, therefore Cooper cannot teach that the "interface depicts anomalies that were used to classify the event."

(2) Claims 10-14 and 18 are patentable over Cooper and Symantec, and Billhartz.

Claims 10, 11 and 13

For the purposes of this appeal only, claims 10, 11 and 13 stand or fall together. Appellant's claim 10 is representative of this group of claims.

Claim 10 includes the features of "... providing ... a list of events identified ..., within the list of events being information indicating event severity, ... determined for an event, by the event having a percentage relationship to an established threshold for issuing an event notification.... ; and providing on a graphical user interface a snooze control to allow a user to snooze future alerts related to the selected event.

In addition to the features discussed for claim 1 above, claim 10 includes the feature "with event severity determined for an event, by the event having a percentage relationship to an established threshold for issuing an event notification." Claim 10 is allowable at least for the reasons discussed in claim 1.

Moreover, Billhartz does not cure deficiencies of the combination of references. The examiner argues that:

Independent claim 10 is rejected using the same basis of arguments used to reject claim 1 above. However, Cooper and Symantec do not explicitly teach an event severity having a percentage relationship to an established threshold for issuing an event notification. This is taught throughout Billhartz though, such as in col. 8 line 41 to col. 9 line 10.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include basing event notifications on percent relationships. One of ordinary skill in the art would have been motivated to perform such an addition to provide greater certainty when issuing alerts, thereby reducing false positives. As indicated in col. 2 liens 15-23 of Billhartz, the previous intrusion detections systems do not reliably indicate whether some nodes are rouge or legitimate nodes.

Billhartz col. 8, line 41 to col. 9, line 10, as understood, discloses determination of a threshold number of collisions of packets to detect intrusions into the network. While Billhartz mentions that: "**the threshold number may be based upon a percentage of a total number of monitored packets having the predetermined packet type ... , then the intrusion alert may be generated,**" the claimed feature is to event severity determined for an event by the event having a percentage relationship to an established threshold for issuing an event notification and not to packet collisions as taught by Billhartz. Accordingly, Billhartz does not suggest the claimed feature.

Claim 12

Claim 12 further distinguish claim 10 over the cited art. Claim 12 includes analogous features as claim 2, and therefore further distinguishes over the alleged combination of references for analogous reasons discussed for claim 10 and claim 2.

Claim 18

Claim 18 includes the feature of "... displaying event details including destination and source fields populated with IP addresses and role classification of the host in the network."

The examiner argues that:

As per claim 18, as best understood by the Examiner, details of source and destination populated with IP addresses is taught throughout Cooper, as can be seen in Figures 23. Cooper then teaches the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158.

Appellant disagrees. Claim 18 further distinguishes over Cooper taken with Symantec, because, not only does claim 18 require displaying event details including destination and source fields populated with IP addresses, it also requires displaying of "role classification of the host in the network." The examiner argues that Cooper teaches role classification at [0100 and 0158], where Cooper discusses a policy generator. As described by Cooper "**The [policy generator] wizard enables the end user to generate policy based on what can be considered gross characteristics of a network at the IP level, such as, for example, policy domains, communities of hosts, servers, subnets and firewalls, as well as at the UDP/TCP service level.**" That is however not the claimed role classification.

Cooper's alleged teaching of "**the preventing of unnecessary alerts due to roles of hosts, such as in paragraphs 100 and 158.**", taken with the alleged teaching of **event details including destination and source fields populated with IP addresses,** does not suggest all of the features of claim 18 at least because Cooper does not display the policy or role classification in Fig. 9.

(3) Claims 15-17 and 21 are patentable over Cooper, Symantec, Billhartz, and Porras.

Claims 15-17 and 21 are allowable at least for the reasons discussed in claim 10.

(4) Claim 19 is patentable over Cooper, Symantec, Billhartz, and Central Point.

Claim 19 is allowable at least for the reasons discussed in claim 10.

(5) Claim 20 is patentable over Cooper, Symantec, Billhartz, and Kuroshita.

Claim 20 is allowable at least for the reasons discussed in claim 10.

Conclusion

Appellant submits that claims 1-25 are allowable over the art of record. Therefore, the examiner erred in rejecting Appellant's claims and should be reversed.

Respectfully submitted,

Date: August 8, 2008

/Denis G. Maloney/
Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

21996297.doc

Appendix of Claims

1. A graphical user interface rendered on a display associated with an intrusion detection system, the graphical user interface comprising:

a field that depicts a summary of anomalies identified as part of an event that is detected in a network, the summary indicating event severity details of the event; and

an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time.

2. The graphical user interface of claim 1 wherein the snooze control feature is selected based on event types and roles of hosts.

3. The graphical user interface of claim 1 further comprising:

a control to allow a user to clear an alert if the alert appears on an overview page that provides an operator with an aggregated view of network status.

4. The graphical user interface of claim 3 wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event.

5. The graphical user interface of claim 1 wherein details of events include values of source, destination, and protocol that caused an event to be raised.

6. The graphical user interface of claim 1 wherein event severity is coded by an indicia.

7. The graphical user interface of claim 1 wherein the interface includes a control to clear a selected alert.

8. The graphical user interface of claim 1 wherein the interface includes a details control that allows a user to observe details about a selected anomaly.

9. The graphical user interface of claim 1 wherein the details control presents a list of IP addresses to which a host attempted to connect to.

10. A method comprises:

providing an operator with a list of events identified by an intrusion detection system, within the list of events being information indicating event severity, with event severity determined for an event, by the event having a percentage relationship to an established threshold for issuing an event notification;

displaying details of a selected one of the events to a user; and

providing on a graphical user interface a snooze control to allow a user to snooze future alerts related to the selected event.

11. The method of claim 10 the snooze control allows an event to be snoozed for a fixed period of time.

12. The method of claim 10 wherein the snooze control is for selected event types and roles.

13. The method of claim 10 further comprising:

clearing a selected alert from the list of events.

14. The method of claim 13 further comprising:

displaying anomalies that were used to classify the event.

15. The method of claim 14 further comprising:

displaying event details that indicate historically normal operating conditions of a host and current operating conditions of a host to allow the operator to take an appropriate action.

16. The method of claim 15 wherein one of the operating conditions displayed is normal and current connection rates of the host.

17. The method of claim 15 wherein the type of events include worm propagation, unauthorized access, denial of service attacks, and historical anomaly.

18. The method of claim 10 further comprising:

displaying event details including destination and source fields populated with IP addresses and role classification of the host in the network.

19. The method of claim 10 further comprising:

displaying actions taken by the operator for the particular event.

20. The method of claim 10 further comprising:

displaying network statistics associated with network flows; and

displaying a ranking of hosts in the network according to a network statistical measure.

21. The method of claim 20 wherein the network statistics are a number of bytes per second and packets per second of each type of protocol observed in the system.

22. A computer program product residing on a computer readable medium for producing a graphical user interface for an intrusion detection system, the computer program product comprising instructions for causing a computer to:

render a graphical user interface on an output device, the graphical user interface comprising:

a field that depicts a summary of anomalies identified as part of an event that is detected in a network, the summary indicating event severity details of the event;

an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time.

23. The computer program product of claim 22 wherein the snooze control is selected based on event types and roles of hosts.

24. The graphical user interface of claim 22 further comprising instructions to render in the graphical user interface:

a control to allow a user to clear an alert if the alert appears on an overview page that provides an operator with an aggregated view of network status.

25. The computer program product of claim 22 wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event.

Evidence Appendix

NONE

Related Proceedings Appendix

NONE